REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03052010	FINAL	

4. TITLE AND SUBTITLE

U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

David M. Franklin, Major, USAF

Paper Advisor: Roy S. Petty, CAPT, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT. The character of cyberspace, the requirement to share situational awareness, and a need for coordination of cyber effects crossing geographic areas of responsibility (AORs) has driven continued centralization of cyberspace command and control (C2). This centralization confronts traditional command relationships and will likely generate friction between the future Commander, U.S. Cyber Command (CDR USCYBERCOM) and Geographic Combatant Commanders (GCCs). Easing of friction requires a careful balance of equities between these Joint Force Commanders (JFCs) and must provide for global unity of effort while not significantly constraining the GCC's freedom of action in the cyber domain. To achieve this balance, the Department of Defense (DOD) should specify establishment, exercise and institutionalization of a Cyber Coordination Authority (CCA). CCA will define, through DOD establishing directives, detailed authorities used by supported and supporting combatant commanders to adequately plan, prepare, and control reach back cyber capabilities organic to USCYBERCOM. To exercise CCA on behalf of the GCC, a Director of Cyber Forces (DIRCYBERFOR) is required to advise, coordinate, integrate and perform staffing functions to weave robust cyber effects throughout the GCC's major lines of operations. CCA requires institutionalization within joint and service doctrines to legitimize cyberspace as a warfighting domain, formalize cyberspace operations, and provide an effective forum to advocate for resources.

15. SUBJECT TERMS

Cyberspace, Command and Control (C2), Command Relationships, Coordinating Authority, USCYBERCOM, Doctrine

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Department
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		**34**	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority

by

DAVID M. FRANKLIN

Major, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

03 May 2010

Contents

List of Illustrations

Abstract

U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority

The character of cyberspace, the requirement to share situational awareness, and a need for coordination of cyber effects crossing geographic areas of responsibility (AORs) has driven continued centralization of cyberspace command and control (C2). This centralization confronts traditional command relationships and will likely generate friction between the future Commander, U.S. Cyber Command (CDR USCYBERCOM) and Geographic Combatant Commanders (GCCs). Easing of friction requires a careful balance of equities between these Joint Force Commanders (JFCs) and must provide for global unity of effort while not significantly constraining the GCC's freedom of action in the cyber domain. To achieve this balance, the Department of Defense (DOD) should specify establishment, exercise and institutionalization of a Cyber Coordination Authority (CCA). CCA will define, through DOD establishing directives, detailed authorities used by supported and supporting combatant commanders to adequately plan, prepare, and control reach back cyber capabilities organic to USCYBERCOM. To exercise CCA on behalf of the GCC, a Director of Cyber Forces (DIRCYBERFOR) is required to advise, coordinate, integrate and perform staffing functions to weave robust cyber effects throughout the GCC's major lines of operations. CCA requires institutionalization within joint and service doctrines to legitimize cyberspace as a warfighting domain, formalize cyberspace operations, and provide an effective forum to advocate for resources.

Introduction

It must be remembered that there is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than the creation of a new system.

— Niccolo Machiavelli, The Prince and the Discourses

Increasingly, command relationships in cyberspace are being replaced by or intermixed with different types of arrangements: alliances, coalitions, inter-agency partnerships, and coordination authorities. In these non-traditional relationships no one organization commands or controls. Successful relationships in this paradigm must be based on unity of effort through cooperation and common understanding of objectives. The character of cyberspace, the requirement to share situational awareness, and a need for coordination of cyber effects crossing geographic areas of responsibility (AORs) has driven centralization of cyberspace command and control (C2) away from Geographic Combatant Commanders (GCCs) towards United States Cyber Command (USCYBERCOM). This centralization confronts traditional command relationships and will likely generate friction between the future CDR USCYBERCOM and GCCs. Easing of friction requires a careful balance of equities between Joint Force Commanders (JFCs) and must provide for global unity of effort while not significantly constraining the GCC's freedom of action in the cyber domain. To achieve this balance, the Department of Defense (DOD) should specify establishment, exercise and institutionalization of a Cyber Coordination Authority (CCA). CCA would define, through DOD establishing directives, detailed authorities needed by supported and supporting combatant commanders to adequately plan, prepare, and control reach back cyber capabilities.

Background

The cyberspace domain and its related technologies present extraordinary opportunities for the GCC. Rapid exploitation of these opportunities has revealed alarming vulnerabilities and dependencies. GCCs rely almost exclusively on technologies in cyberspace to move information to decision makers, commanders, and troops giving combatant commanders unparalleled abilities to observe, orient, decide and act. However, the ability to work through cyberspace interruptions via redundancy, consequence management, restorative capacity, and continuity of operations procedures is negligible.[1] Due mostly to budgetary constraints, the U.S. has moved away from robust, hardened, stand-alone systems and turned to less costly commercial off-the-shelf technologies (COT) unencumbered by lengthy DOD development processes. Streamlined procurement and cost savings are largely the result of the commingling of civilian and military cyberspace infrastructure and technologies.[2] These technologies are not designed to operate in contested environments and generate significant risks to GCCs. However, addressing these risks is beyond the scope of this paper.

Effectively attending to this new global dimension of risk was the impetus for a recent Department of Defense (DOD) reorganization. USCYBERCOM, a new sub-unified command, was established to secure U.S. freedom of action in cyberspace.[3] Defense Secretary Gates' June 23, 2009 Establishment Memorandum directed the Commander, United States Strategic Command (CDR USSTRATCOM) to delegate authority to conduct specified cyberspace operations of the Unified Command Plan (UCP) to the CDR USCYBERCOM.[4] Secretary Gates stated:

> The Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations.

> Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.

Almost a year after publishing this memorandum and a mandated October 2010 Full Operating Capability (FOC), the implementation plan delineating USCYBERCOM's C2 and support relationships with GCCs, Services, and other U.S. Government departments has yet to be approved by the Office of the Secretary of Defense (OSD).[5] Selection of cyber command relationships must sew together critical C2 seams exposed by the global nature of cyberspace to mitigate adversary exploitation. Cyber command relationships must also carefully balance organizational equities, as they will determine how much authority USCYBERCOM exercises in planning, preparing, executing and controlling cyberspace operations in the GCC's area of responsibility (AOR). Finding this balance promises to be contentious as it will confront traditional command relationships.

Confronting the Command Relationship Status-Quo

I often hear claims of "it's my network". No it's not; it's an integral part of the entire network, and vulnerability in your network is vulnerability in the entire GIG.

— General Kevin P. Chilton Commander, United States Strategic Command

The character of the cyberspace domain challenges traditional authorities exercised by GCCs and will likely create friction points in future command relationship definition with USCYBERCOM. The 2008 UCP establishes six geographic combatant commands and assigns missions, responsibilities, and geographic boundaries through definition of AORs (Figure 1).[6] Within these geographic AORs, GCCs provide authoritative strategic direction. GCCs assign missions, establish rules of engagement, and develop constraints and restraints through exercise of combatant command authority (COCOM) as defined in Title 10 of the

U.S. Code (USC) Section 164(c)(1). Additionally, the GCC defines policies and concepts of operations for integration into operation plans (OPLANs).[7] Under the established construct, GCCs assign tasks, forces, and resources to meet their designated objectives, but the non-linear domain of cyberspace challenges this conventional architecture.

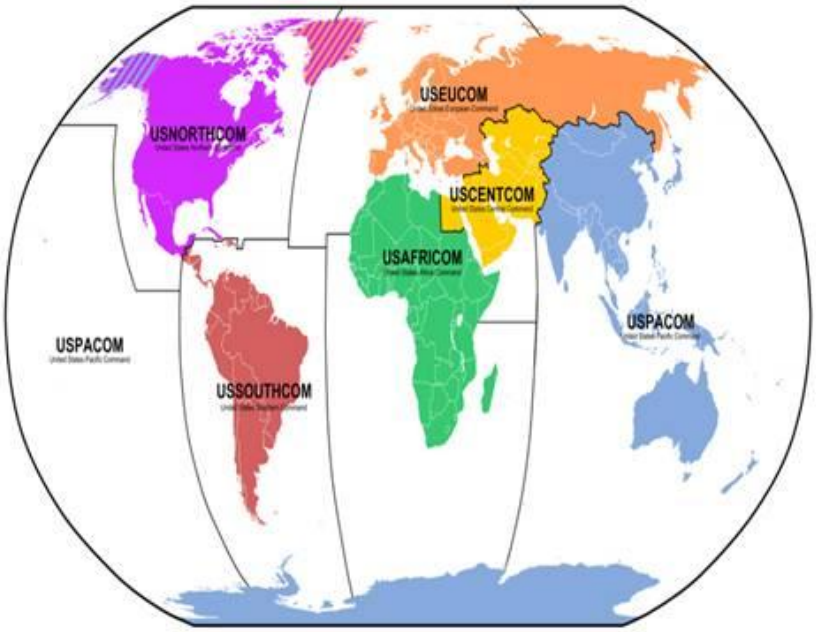

Figure 1: Geographic Combatant Commands[8]

The global nature of cyberspace complicates command relationship paradigms, making the traditional model less than optimal for C2 of operations within the cyber domain.[9] At the core of the issue is the fact that cyberspace is interconnected: militaries, governments, the civilian sector, and the rest of the world. This makes coordinating operations in the cyber domain, at the local and global levels, incredibly complex and fraught with new and challenging problems. Cyber attacks are not traditional point-to-point attacks traveling through a single GCC's AOR. Moreover, digital information travels, almost instantaneously, through multiple AORs, hindering the ability to recall cyber attacks and making their effects sometimes irreversible and uncontrollable once launched.[10] These

characteristics diminish the relevancy of geographic borders and blur AOR responsibilities complicating who responds, takes the lead, and coordinates actions to ensure unity of effort in the cyber domain. Additionally, ambiguity surrounding consequences of offensive cyber operations further complicates responsibilities for decentralized execution. The likelihood of tactical or operational actions in cyberspace having strategic effects is a real and credible concern. Computer network attacks possess a potential to lead to unanticipated cascade effects. Second and third order effects resulting from cyber attacks on untargeted systems are sometimes impossible to anticipate or counter and can infringe on national sovereignty or inadvertently target civilian cyber infrastructure.[11] Subsequent reprisals or unintended escalation resulting from these types of operations elevates the required approval authorities to execute offensive cyber operations within an AOR to reside with the National Security Council (i.e., SECDEF and President) instead of with the GCC.[12] To effectively address these issues, provide shared cyberspace situational awareness, and conduct defense of DOD networks, a new organization was established to secure U.S. freedom of action in the domain.

The USCYBERCOM Imperative

Maintaining freedom of action in cyberspace in the 21st century is as inherent to U.S. interests as freedom of the seas was in the 19th Century and access to air and space in the 20th Century.

— Lieutenant General Keith Alexander Director, National Security Administration

Due to the U.S. military's growing vulnerability and dependence on net-centric activities in cyberspace, the DOD required an organization with a single focus on

maintaining U.S. freedom of action in the cyber domain (Figure 2).[13] The creation of a single, sub-unified cyber command provides the DOD with a command comprised of forces

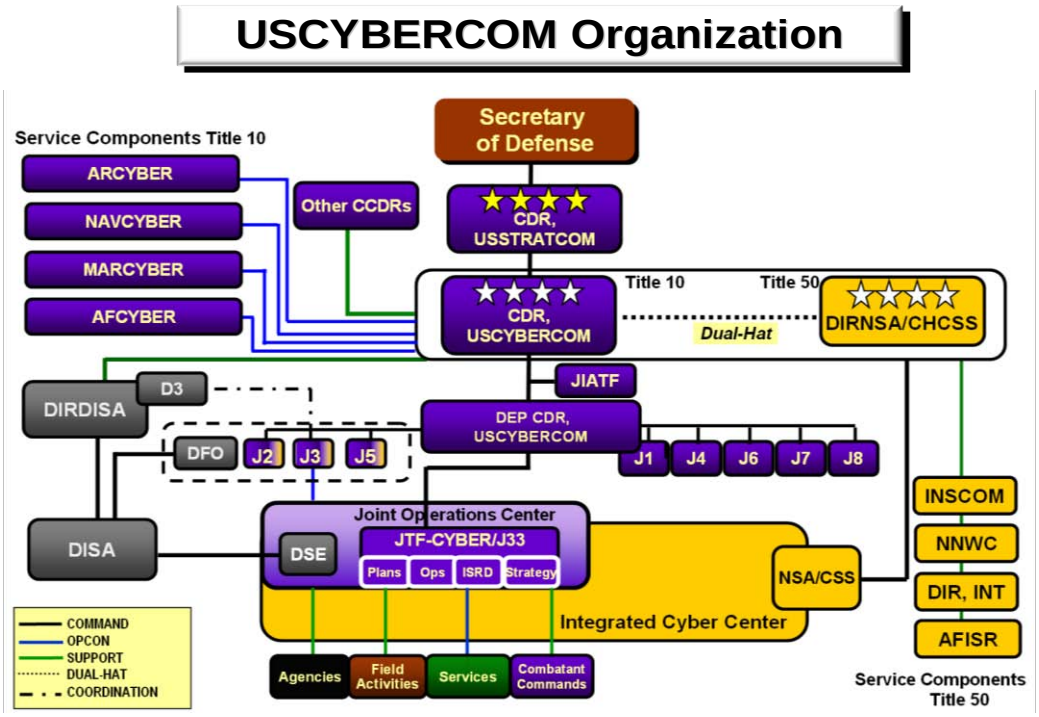

Figure 2: Proposed United States Cyber Command Organization[14]

and capabilities aligned to conduct cyber operations and overcome challenges presented by the global nature of the domain. Command establishment reflects the desire of the DOD to centralize cyber operations, address the non-traditional complexities inherent to the domain, and elevate computer network security as a national security issue through creation of a new command.[15] USCYBERCOM will be formed by the merger of Joint Functional Component Command Network Warfare (JFCC-NW) and Joint Task Force-Global Network Operations (JTF-GNO) which will both de-activate in October 2010 upon USCYBERCOM FOC.[16] This union brings together existing offensive and defensive capabilities under one organization to defend and attack critical military capabilities in cyberspace.[17] USCYBERCOM's primary

role will be to accomplish cyber integration globally through centralized planning, coordination, and execution of offensive and defensive cyberspace operations.[18] As continued cyberspace C2 centralization occurs within DOD, with USCYBERCOM as its lead agency, establishing directives need to define command relationships and coordinating authorities which balance GCC equities and drive responsive mechanisms to focus cyber power on global as well as theater requirements.[19]

Balancing the Equities

The United States can achieve superiority in cyberspace only if supported and supporting relationships are clearly defined and executed.

— The National Military Strategy for Cyberspace Operations

The 2010 Quadrennial Defense Review calls for continued C2 centralization of cyber operations under CDR USCYBERCOM.[20] However, this centralization fuels unresolved questions on how USCYBERCOM will balance equities with GCCs to ensure responsive integration, deconfliction, and synchronization of global cyberspace operations within their respective AORs. As a basis for support, Secretary Gates' USCYBERCOM Establishment Memorandum directs USCYBERCOM to establish and maintain direct liaison (DIRLAUTH) with combatant commands, Services, and DOD agencies. However, DIRLAUTH is more applicable to planning than operations and is a coordination relationship, not an authority through which command may be exercised.[21] The specific mechanism through which C2 of operational cyber forces will be executed requires definition.

The DOD establishing directive must clearly define supported and supporting relationships between USCYBERCOM and combatant commanders. Formal documentation will help integrate cyber operations into all mission areas and enhance DOD cyberspace

collaboration. An establishing directive, as stipulated in *Joint Publication 1, Doctrine for the Armed Forces* (JP-1), is an order specifying the purpose and methods used in a support relationship.[22] DOD establishing directives for cyber should specify a direct support relationship requiring USCYBERCOM to support GCCs and direct USCYBERCOM forces to answer directly to the GCC's request for assistance through detailed coordination authorities.[23] This directive should specify CDR USCYBERCOM as the supported commander for planning, leading, and conducting DOD defensive cyber and global network operations (computer network defense). USCYBERCOM is uniquely aligned to conduct these functions and possesses appropriate C2 mechanisms and the preponderance of cyber forces to accomplish the assigned tasks within the domain.[24] Additionally, USCYBERCOM should be the supporting commander for offensive cyber missions (computer network exploitation and attack). GCCs should maintain authoritative control over the timing and tempo of cyber effect generation within their AORs in order to synchronize cyberspace operations into their concepts of operation. The establishing directive should specify detailed capabilities (e.g., CNA, CND, and CNE), effects, as well as scope and duration of the actions to be taken by USCYBERCOM in support of GCCs. These directives require sufficient specificity in coordinating authority as to eliminate potential friction points caused by the unique cyberspace operating environment.

Friction points in any future establishing directive become evident between USCYBERCOM and GCCs when examining forces allocated to the supporting effort. Cyber forces dedicated to the GCC's objectives in the cyber domain may not fall under the GCC's operational control (OPCON). If this is the case, USCYBERCOM will determine apportionment and prioritization of cyber resources consistent with available assets and

requirements of all assigned tasks and global priorities from other GCCs. As the central adjudicator, CDR USCYBERCOM will make allocation decisions which may become divisive when multiple GCCs require cyber support and must compete for limited resources. Furthermore, USCYBERCOM's authority to modify a supporting effort, in the event of an exceptional opportunity or emerging priority, can complicate a GCC's operational synchronization. This can put at risk achievement of his objectives.[25]

Finally, a GCC's lack of control in the gain-loss process during the conduct of cyber operations in their AORs may limit freedom of action while prosecuting certain targets. CDR USCYBERCOM will also be "dual-hatted" as the Director of the National Security Administration (NSA), which, like all intelligence agencies, could be naturally expected to seek to protect sensitive sources and methods.[26] In the conduct of cyber operations, both the GCC and the CDR USCYBERCOM must jointly decide whether the intelligence value of gaining information from a target is worth more than the value of destroying that target. Within a geographic operational area, this decision usually rests solely with the GCC, confronting his traditional authority. A process for conflict resolution must be carefully considered to balance JFC equities in this gain-loss assessment to meet both global and theater cyber requirements.

The need to balance these equities will require USCYBERCOM and GCCs to construct responsive, simple, and flexible command relationships based on well defined coordinating authorities. Coordination authorities in cyberspace must be exercised by agile organizations affording high-tempo cyber operations, communication networks, and assured access to cyberspace to the GCC.[27]

Cyber Coordinating Authority (CCA) Establishment, Exercise and Institutionalization

We do not conduct activities in the new domain of cyberspace for convenience; we conduct them out of necessity. That makes successful operations in cyberspace everyone's business—especially leaders and commanders [GCCs].

— General Kevin P. Chilton Commander, United States Strategic Command

To comply with Secretary Gates' June 2009 mandate directing development of USCYBERCOM's "C2, reporting, and support relationship with combatant commands," DOD establishing directives should specify creation of a Cyber Coordination Authority and stipulate detailed supported and supporting relationships between USCYBERCOM and GCCs.[28] The concept of coordinating authority is not new and is defined in JP-1, but CCA has distinctions requiring explanation. The notion of CCA emulates the space domain's Space Coordinating Authority (SCA).[29] Space and cyber domains share many similarities. As war fighting domains, air, land, and sea are largely defined by geography or range of operation. Space and cyber are cross-cutting domains, enabling the three other finite spatial domains through faster decision making.[30] The domains are global in scope and indifferent to physical terrain or lines drawn on a map with near instantaneous effects transmitted through their domains.[31] Both cyber and space are global commons vital to civil and commercial activities and essential to the economy and military operations. These domain characteristics generate similar challenges when attempting to define command relationships, C2 structures, and balancing equities between supported and supporting commanders. Because of these similarities, command relationships for U.S. military space operations may be used as a template for establishing cyber command relationships while keeping in mind that cyber C2 is unique and will drive distinctive features of command relationships in the cyberspace.

Under this construct, combatant commanders assigned a geographic area of responsibility by the UCP are also assigned the role of the CCA in the operational area. The CCA is responsible for coordinating joint cyberspace operations with CDR USCYBERCOM to integrate CNO capabilities into theater OPLANs (Figure 3). A more precise definition

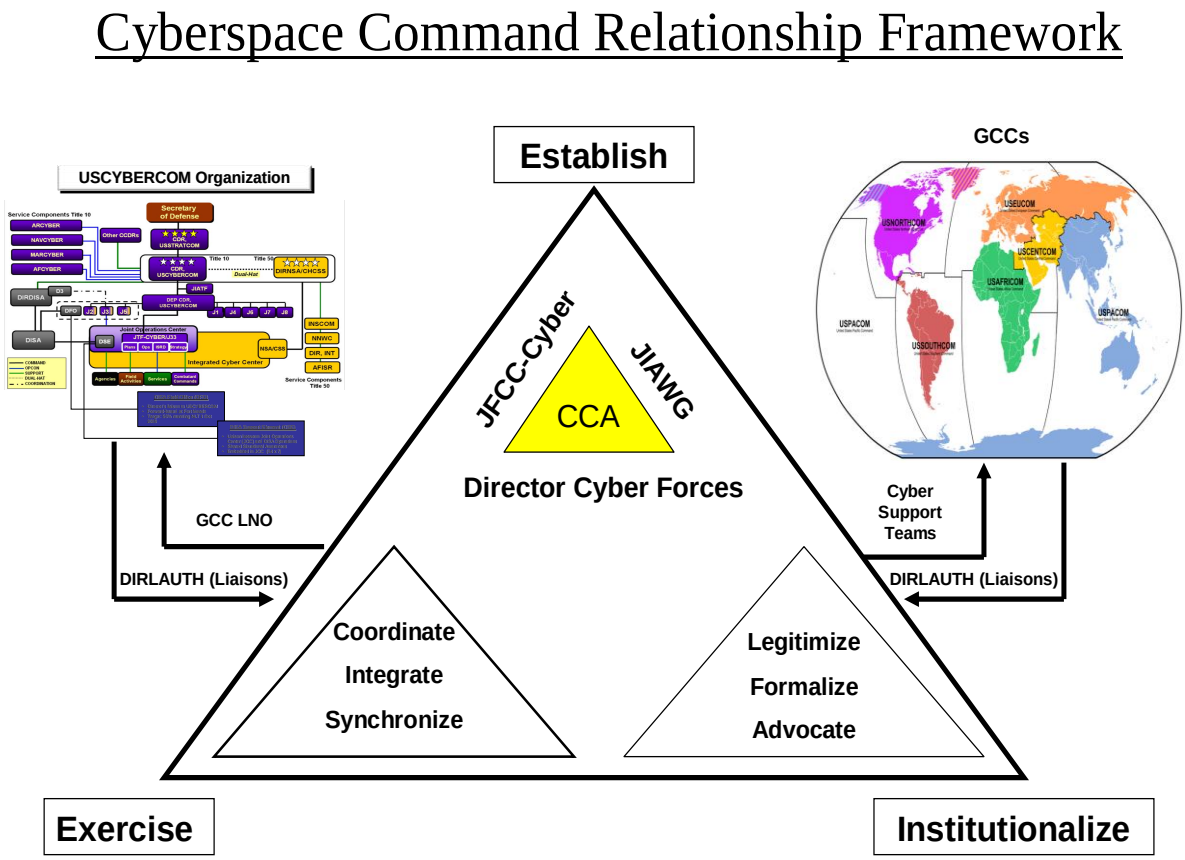

Figure 3: Cyberspace Command Relationship Framework

blending the JP-1 definition of coordinating authority and the proposed cyber definition would read as follows:

> A GCC assigned responsibility for coordinating joint cyberspace operations and integrating cyberspace capabilities in the operational area or activities involving forces of two or more Military Departments, two or more joint force components, or two or more forces of the same Service. The GCC has the authority to require consultation between agencies involved, but does not have the authority to compel

> agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority (i.e., USSTRATCOM and then SecDef). CCA is a consultation relationship, not an authority through which command may be exercised.[32]

As proposed, the CCA would be responsible for coordinating and integrating cyber capabilities in its AOR. This authority continues to provide each GCC with full strategic direction in his AOR and control over timing and tempo for theater cyber efforts. This framework provides the CCA primary responsibility for synchronizing joint cyber effects into their concept of operations. This includes determining and assembling theater cyber requirements within the AOR which can be satisfied by reach back cyber capabilities organic to USCYBERCOM. The CCA provides a prioritized list of cyber requirements based on his objectives to CDR USCYBERCOM for planning and execution of assigned missions. To ensure prompt and timely compliance, CDR USCYBERCOM and CCAs should approve DIRLAUTH with each other's staffs.

As the global CCA, CDR USCYBERCOM should establish a Joint Force Component Commander-Cyber (JFCC-C) as stipulated in *Joint Publication 3-0, Joint Operations.*[33] For cyber related activities, the JFCC-C would be the primary USCYBERCOM interface to supported GCCs and exercise OPCON of assigned cyber forces. The JFCC-C would reside at USCYERCOM and conduct full spectrum military cyberspace operations from USCYBERCOM's Integrated Cyber Center. Under this proposal, JFCC-C would serve as the single point of contact for military cyber operational matters, including planning, tasking, directing, and executing cyber operations using assigned cyber forces and resources. This construct will enhance cyber unity of effort through centralized sharing of situational awareness and coordination of cyber effects crossing AOR boundaries.

Under this proposal, each GCC should appoint a DIRCYBERFOR to exercise CCA responsibilities on his behalf. The DIRCYBERFOR concept is derived from joint doctrine, analogous to a Director of Mobility Forces (DIRMOBFOR) or Director of Space Forces (DIRSPACEFOR), and satisfies a domain specific coordination function for the CCA.[34] A DIRCYBERFOR provides senior officer cyberspace expertise for the CCA and coordinates reach back cyber capabilities organic to USCYBERCOM.[35] A DIRCYBERFOR performs cyber related staffing functions coordinating tasks, forces and resources to meet the GCC designated objectives. These activities occur from a Cyber Cell separate and distinct from the Information Operations Cell, although it is recommended that CCA be exercised by the DIRCYBERFOR from the CCA's J-3 directorate.

The DIRCYBERFOR position should be filled with a fully qualified joint officer (JQO with broad cyber expertise in operations, intelligence, and communications. The selection of a DIRCYBERFOR should be a careful decision by the CCA who will grant broad coordination authority to manage his cyber interests. The DIRCYBERFOR is not a command position, but fills a coordinating role only. The DIRCYBERFOR's primary function is to advise the CCA and coordinate planning and execution efforts for cyber operations in the AOR. Under this proposal, cyber support requests submitted by the DIRCYBERFOR, on behalf of the GCC, will drive USCYBERCOM apportionment decisions to determine and assign resources devoted to the CCA's theater cyber efforts. Inherent to this relationship is DIRLAUTH with USCYBERCOM and the proposed JFCC-C.

The use of existing management structures such as a Joint Interagency Coordination Group-Cyber[36] will compliment this construct and encourage collaboration at the operational level with military, USG civilian agencies, and departments.[37] CCA will also be exercised

by the DIRCYBERFOR through exchange of Cyber Liaison Officers (C-LNO). Cyber Support Teams (CST) will be resident in GCC's AOR and GCC LNOs will reside in USCYBERCOM's Integrated Cyber Center (ICC). These liaisons will maintain critical lines of communication between USCYBERCOM and the DIRCYBERFOR helping to enhance interoperability between organizations. Liaison exchanges will be instrumental in mutual understanding of requirements and available resources between USCYBERCOM and the various CCAs.[38]

Counter Argument

GCCs may argue that the need for a coherent cyber campaign within the AOR demands decentralized planning, execution and control of cyber forces from within theater. The growing importance of operations within the cyber domain warrants a local commander with full authority to regulate forces and functions and execute the GCC's intent. This requires the creation of a Joint Force Cyber Component Commander (JFCyCC) as stipulated in JP 3-0.[39] The JFCyCC would reside in the AOR and operate with the other joint force component commanders for air, land, and sea. The JFCyCC would act as the GCC's single cyber integrator assigning missions, tasks, forces, and resources to meet the GCC's designated cyber objectives. Failure to have this decentralized control within the theater puts at risk the GCC's ability to defend and attack critical military capabilities and weakens his capacity to influence adversary decision making and restricting his freedom of maneuver.[40] Cyber forces should be deployed forward to the GCC's AOR and organic cyber forces within theater should be allocated to the JFCyCC who would exercise OPCON and TACON of those forces.

Rebuttal

While joint force component commanders are established by joint doctrine, two significant obstacles exist impeding any efficiencies or enhanced unity of effort gained by the establishment of a JFCyCC. The first obstacle involves approval authorities for cyber weapons release.[41] As previously discussed, the likelihood of tactical or operational actions in cyberspace having strategic, legal and national policy implications is a significant concern. The potential of a cyber operation generating a weapon of mass effect (WME) and the subsequent reprisal or escalation resulting from that operation elevates approval authorities for such operations to the National Security Council.[42] This negates the foundational doctrinal purpose for the establishment of a functional component commander which is to provide decentralized execution of operations within his assigned domain.

Additionally, due to significant human resource limitations and burgeoning global CNO requirements, centralized adjudication of apportionment decisions for cyber forces will become critical. The DOD cyberspace enterprise currently does not possess appropriate resources and numbers of personnel with the training, education, and experience to accomplish assigned cyber missions and may take several years to generate sufficient inventories of both.[43] The determination and assignment of the total expected effort, by percentage and priority, devoted to each GCC cyber operations should lay with the global CCA (CDR USCYBERCOM). Centralized apportionment decisions must be made by CDR USCYBERCOM, who alone has visibility into global resource availability and prioritized requirements. Spreading limited cyber talent amongst six disparate geographic combatant commands diminishes capabilities and global unity of effort in the cyber domain.

Recommendations

We must effectively and efficiently structure forces and associated processes and procedures to execute DOD's priorities in cyberspace.

— Quadrennial Roles and Missions Review Report, January 2009

U.S. military cyber command relationships should be structured to achieve operational commander's objectives through unity of effort. This should be accomplished in the cyber domain through the formal establishment of a CCA between GCCs and the CDR USCYBERCOM (Figure 4). The CCA is a combatant commander assigned a geographic

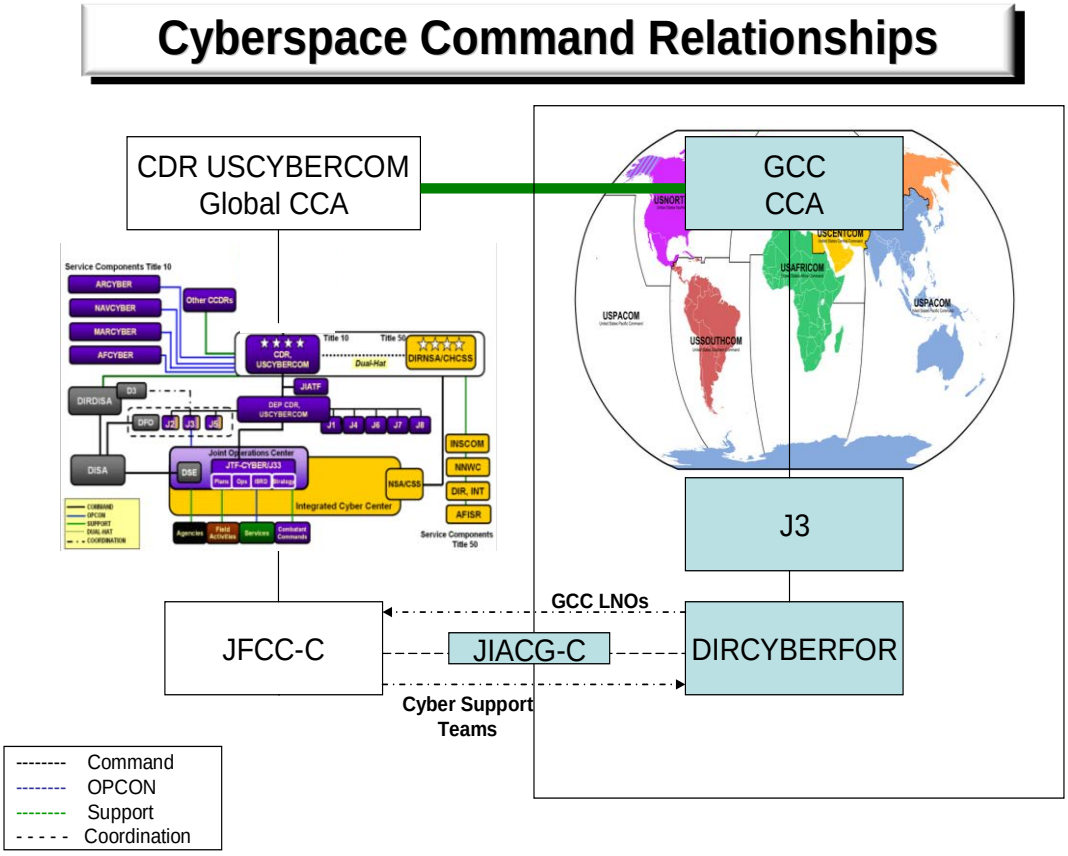

Figure 4: Proposed Cyberspace Command Relationships

area of responsibility by the UCP. The GCC exercises execution of CCA through a Director of Cyber Forces (DIRCYBERFOR). The DIRCYBERFOR advises the GCC and coordinates, integrates and performs staffing functions to harness reach back cyber capabilities organic to

USCYBERCOM. As the global CCA, USCYBERCOM should establish a Joint Force Component Commander-Cyber (JFCC-C) to serve as the single point of contact for military cyber operational matters, including planning, tasking, directing, and executing cyber operations using assigned cyber forces. For cyber related activities, the JFCC-C will be the primary USCYBERCOM interface to supported commanders. The DIRCYBERFOR interfaces with JFCC-C and his staff to conduct coordination, integration and staffing activities tailoring cyberspace operations support to the CCA. Existing management structures (e.g., Joint Interagency Coordination Groups) are leveraged providing the DIRCYBERFOR the ability to collaborate at the operational level with other USG civilian agencies and departments on behalf of the GCC. Cyber LNOs from the supported commander and Cyber Support Teams (CST) from USCYBERCOM are also exchanged to enhance interoperability between USCYBERCOM and supported commanders.

The concept of CCA and the role of the DIRCYBERFOR require institutionalization within joint and service doctrines. Codification of these unique authorities will help legitimize cyberspace as a war fighting domain, aid in formalizing cyberspace operations, and provide an effective forum to advocate for resources. Inclusion of cyberspace command relationships into joint doctrine will provide a common point of reference, terminology, and understanding of the domain's inherent value between supported and supporting commanders. This will drive improved cyber-interoperability resulting in enhanced joint warfighting capabilities and facilitating generation of joint tactics, techniques and procedures.[44]

The role of CCA and DIRCYBERFOR should also be exercised in joint war games and training scenarios with robust cyber domain inputs to help formalize cyberspace

operations and instill "cyber mindedness" into the joint warfighting ethos.[45] Finally, institutionalization of the cyber domain within joint doctrine provides an effective forum to advocate for resources. Successful articulation to the joint community of critical vulnerabilities caused by unprotected networks, as well as the potent capabilities brought to bear by CNO, represent powerful operational requirements. The DOD maintains the largest computer network in the world with USCYBERCOM leading funding advocacy to protect DOD interests in cyberspace as a domain.[46] However, GCC's are influential stakeholders in the Planning, Programming, Budgeting and Execution (PPBE) process. Empowering GCCs with CCA gives them active roles in positive cyberspace funding outcomes. Influence on how forces will be designed, trained, and equipped to protect their information and defend and attack networks in their AORs will translate into more vigorous advocates for cyber funding.

Conclusion

The only thing harder than getting a new idea into the military mind is getting an old one out.

— Captain Sir Basil Liddell Hart

The 2010 QDR established a Department of Defense imperative to operate effectively in cyberspace: "The security environment demands improved capabilities to counter threats in cyberspace…modern armed forces simply cannot conduct effective high-tempo operations without resilient, reliable information and communication networks and assured access to cyberspace."[47] Underpinning the required capabilities alluded to in the QDR are flexible, responsive and balanced command relationships fostering unity of effort in cyberspace through coordination. The character of the cyber domain challenges normal conventions in the development of command relationships which produces potential seams for adversary

exploitation. This paper serves to focus attention on the critical seam in cyberspace C2. As demonstrated, the answers are not simple and require coordination between supported and supporting combatant commanders. Whatever form these relationships take, they must reflect our increasing dependencies amid rising threats to our systems in the cyber domain.

The stand-up of USCYBERCOM in September of 2009 was a major milestone in the evolution of cyberpower. Centralized information gathering, decision making, and execution of operations in cyberspace by USCYBERCOM will improve DOD's cyber capabilities. However, equities between USCYBERCOM and GCCs must be carefully balanced to ensure global unity of effort without limiting the GCC's freedom of action. To adequately address this balance of equities, DOD establishing directives should provide for the establishment, exercise and institutionalization of CCA. Adoption of this construct will help USCYBERCOM generate responsive C2 mechanisms to focus cyberpower on both global and theater cyber requirements.

GLOSSARY

Centralized Control — Placing within one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations. (JP 3-30)

Combatant Command (command authority) — Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM. (JP 1-02)

Combatant Commander — A commander of one of the unified or specified combatant commands established by the President. Also called CCDR. See also combatant command; specified combatant command; unified combatant command. (JP 3-0)

Command — 1. The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual. Also called CMD. (JP 1-02)

Command and Control— The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1)

Command Relationships — The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support. (JP 1)

Coordinating Authority —A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments, two or more joint force components, or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (JP 1-02)

Computer Network Attack (CNA) — Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DODI 3600.02)

Computer Network Defense (CND) — Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DOD information systems and computer networks in response to a CND alert or threat information. (DODI 3600.01)

Computer Network Exploitation (CNE) — Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (DODI 3600.02)

Computer Network Operations (CNO) — Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 1-02)

Cyberspace — A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (NMS-CO)

Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08) (JP 1-02)

Cyberpower —The organized, integrated use of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in and through cyberspace for purposes of foreign policy, strategy, operations, and tactics. (Not included in Joint doctrine)

Cyberspace Coordinating Authority — A commander responsible for coordinating joint cyberspace operations and integrating cyberspace capabilities in the operational area. Also called CCA. (Not included in Joint doctrine)

Cyberspace Effect — A change to a condition, behavior, or degree of freedom within cyberspace. (Not included in Joint doctrine)

Cyberspace Operations — The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (CJCS Memo 19 Aug 2009) (JP 1-02)

Decentralized Execution — Delegation of execution authority to subordinate commanders. (JP 3-30)

Direct Liaison Authorized — That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. Direct liaison authorized is more applicable to planning than operations and always carries with it the requirement of keeping the commander granting direct liaison authorized informed. Direct liaison authorized is a coordination relationship, not an authority through which command may be exercised. Also called DIRLAUTH. (JP 1-02)

Establishing Directive — An order issued to specify the purpose of the support relationship. (JP 3-02)

Global Information Grid (GIG) — The globally interconnected , end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software, data, security services, and other associated services necessary to achieve information superiority. (JP 6-0)

Information Environment (IE) — The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02) (JP 3-13)

Integrated Cyber Center (ICC) — The mission of the ICC is to provide CDR JFCC-Cyber with agile and responsive C2 capabilities to conduct cyber operations on a 24/7 basis. The ICC provides reach back to CCDRs' CCAs. Provides operational-level cyber C2 support to CDR JFCC-Cyber Supports the inter theater responsibilities of CDR JFCC cyber and coordinates with theater CCAs. (Not included in Joint doctrine)

Liaison — That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 3-08)

Line of Operations — 1. A logical line that connects actions on nodes and/or decisive points related in time and purpose with an objective(s). 2. A physical line that defines the interior or

exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s). Also called LOO. (JP 3-0)

Operational Control. Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. See also combatant command (command authority); tactical control. (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

Network Operations — Activities conducted to operate and defend the Global Information Grid (GIG). (JP 1-02)

Support —The action of a force that aids, protects, complements, or sustains another force in accordance with a directive requiring such action. (JP 1)

Tactical Control — Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. Also called TACON. See also combatant command (command authority); operational control. (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

Unity of Effort — Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization — the product of successful unified action. (JP 1) (JP 3-0, A-2)

End Notes

[1] Kamal Jabbour, "*Cyber Vision and Cyber Force Developmen*t," Strategic Studies Quarterly (Spring 2010): 63.
[2] Crowell, Richard. Interview by author. Personal interview. Naval War College, April 29, 2010.
[3] Robert M. Gates, U. S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U. S. Cyber Command Under U. S. Strategic Command for Military Cyberspace Operations*, June 23, 2009.
[4] This 30 September 2008 key strategic document establishes the missions, responsibilities, and geographic areas of responsibility for commanders of combatant commands. In this document USSTRATCOM is assigned the cyberspace mission and recognizes cyberspace as a warfighting domain critical to joint military operations. USCYBERCOM is now responsible for specified cyberspace operations detailed in section 18.d.(3) to include but not limited to directing Global Information Grid operations and defense, planning against designated cyberspace threats and coordinating with DOD, interagency and civilian authorities for cyberspace effects.
[5] In Secretary Gates' 23 Jun 2009 establishment memorandum, the Chairman of the Joint Chiefs of Staff (CJCS) were tasked to issue a planning order directing CDRUSSTRATCOM to develop an implementation plan for USCYBERCOM, to be submitted for his approval by 1 September 2009. The implementation plan was to delineate USCYBERCOM's mission, roles and responsibilities; command and control, reporting and support relationships with combatant commands, Services and U.S. Government departments. After interviewing an undisclosed CJCS representative, the planning order and implementation plan remain in CJCS coordination channels.
[6] Gates, Robert. *Unified Command Plan 2008*. Washington, DC: DOD, 2008.
[7] United States. "Commanders of Combatant Commands: Assignment; Powers and Duties." In *Title 10, United States Code: Armed Forces (as Amended Through December 31, 1996)*. New York: Government Printing Office, 1996. 10 USC Sec. 164.
[8] "Defense.gov Photos: Unified Command Plan Map." United States Department of Defense (defense.gov). http://www.defense.gov/multimedia/multimedia.aspx (accessed April 25, 2010).
[9] Libicki, Martin C. "Cyber Deterrence and Cyberwar." *Rand.org*, 76.
[10] Petty, Roy. Interview by author. Personal interview. United States Naval War College, April 15, 2010.
[11] DNI Blair's comments in an interview with Hadro, Matt. "Conservative News: U.S. A Threat in Cyber War; Financial and Government Activities Vulnerable - HUMAN EVENTS." Conservative News, Views & Books - HUMAN EVENTS. http://www.humanevents.com/article.php?id=35991 (accessed April 9, 2010).
[12] Messmer, Ellen. "U.S. cyber counterattack: Bomb 'em one way or the other." NetworkWorld.com. http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html (accessed April 9, 2010).
[13] CJCS, *The National Military Strategy for Cyberspace Operations*, 9. The NMS-CO states, "DOD force transformation hinges largely on a move toward net-centric operations. Significant investments in force structure, infrastructure, and programs have oriented DOD components toward the use of cyberspace as an integral part of warfighting."

[14] McCullough, Barry. "U.S. Fleet Cyber Command." Speech, Mission Brief from U.S. Tenth Fleet, Maryland, February 22, 2010.
[15] Remarks by Deputy Secretary Lynn at the Center for Strategic and International Studies, Washington, D.C. June 15, 2009.
[16] To accomplish their UCP assigned mission to ensure US freedom of action in cyberspace, USSTRATCOM set up two organizations. The Joint Task Force-Global Network Operations (JTF-GNO) directs the operation and defense of the Global Information Grid to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DOD's full spectrum of war fighting, intelligence, and business missions. JFCC - Network Warfare (JFCC-NW) plans, and when directed, executes operations in and through cyberspace to assure US and allied freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain.
[17] Ibid, 2.
[18] Robert M. Gates, U. S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U. S. Cyber Command Under U. S. Strategic Command for Military Cyberspace Operations*, June 23, 2009.
[19] Cyberpower is defined as the organized, integrated use of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in and through cyberspace for purposes of foreign policy, strategy, operations, and tactics. (Not included in Joint doctrine)
[20] Gates, Robert. *Quadrennial Defense Review Report*. Washington, DC: Department Of Defense, 12 February 2010, ix.
[21] Ibid, IV-13.
[22] Ibid, IV-10
[23] Direct support is defined as a mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. Also called DS. (JP 3-09.3)
[24] Alexander, Keith B. Advance Questions for Lieutenant General Keith Alexander, USA." armed-services.senate.gov. armed services.senate.gov/statement/2010/04%20April/ Alexander%2004-15-10.pdf (accessed April 16, 2010).
[25] Vego, Milan. *Joint Operational Warfare: Theory & Practice*. Newport, RI: Naval War College Press, 2007, IX-145.
[26] There have been many instances in history where military and political leaders had to struggle with the choice of acting on intelligence information to save lives or forestall an enemy success at the cost of the enemy learning that their communications, information, or capabilities had been compromised. These choices are referred to as "gain-loss" calculations. U.S. Cyber Command is to be headed by the Director of the NSA, which, like all intelligence agencies, could be naturally expected to seek to protect sensitive sources and methods.
[27] CJCS, *The National Military Strategy for Cyberspace Operations*, 11.
[28] U.S. Department of Defense. Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. Washington DC: Office of the Secretary of Defense, 23 June 2009.
[29] Space Coordinating Authority is possessed by a commander responsible for coordinating joint space operations and integrating space capabilities in the operational area. Also called SCA. Derived from U.S. Office of the Chairman of the Joint Chiefs of Staff. Space

Operations. Joint Publication (JP) 3-14. Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 6 January 2009. , III-2.
[30] National Military Strategy for Cyberspace Operations (December 2006), 4.
[31] Ibid, 10.
[32] Ibid, IV-13
[33] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations.* Joint Publication (JP) 3-0. Washington, DC: CJCS, 17 September 2006 Incorporating Change 1 13 February 2008, xiv.
[34] The positions of Director of Space Forces (DIRSPACEFOR) and Director of Mobility Forces (DIRMOBFOR) have been used with wide success in CENTCOM, PACOM, SOUTHCOM and EUCOM AORs. The position of DIRSPACEFOR and DIRMOBFOR are codified in JP 3-14, IV-11 and the JP 3-30, xxi respectively.
[35] To exercise CCA on behalf of the GCC, a Director of Cyber Forces (DIRCYBERFOR) is required to advise the GCC. The DIRCYBERFOR should be a senior officer with breadth in cyber activities (communications, intelligence and operations) possessing the requisite skill set to coordinate, integrate and perform staffing functions with other military and civilian stakeholders in the cyberspace enterprise.
[36] The concept of a Joint Interagency Coordination Group-Cyber (JIACG-C) was taken from Major Osvaldo Ortiz, USA, *Joint Interagency Coordination Group-Cyber: Empowering the Combatant Commander Against the No-Border Threat.* (Newport, RI: Naval War College, 2009).
[37] The Joint Interagency Coordination Group (JIACG) is an interagency staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners. Composed of USG civilian and military experts accredited to the combatant commander and tailored to meet the requirements of a supported combatant commander. Derived from U.S. Office of the Chairman of the Joint Chiefs of Staff. *Interagency, Intergovernmental* Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I. Joint Publication (JP) 3-08. Washington, DC: CJCS**,** 17 March 2006, II-17.
[38] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Task Force Headquarters.* Joint Publication (JP) 3-33. Washington, DC: CJCS**,** 16 February 2007, II-17.
[39] Ibid, xiv.
[40] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations.* Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006, I-9.
[41] Ibid, 464.
[42] Weapons of mass effect (WME) are defined as weapons capable of inflicting grave destructive, psychological and or economic damage. Derived from Crowell, Richard M. War in the Information Age: A Primer for Cyberspace Operations in the 21st Century (Newport, RI: Naval War College, 2008).
[43] Baldor, Lolita. "Report: Shortage of Cyber Experts a Big Threat to U.S. Government - InsideTech.com." InsideTech.com: The IT Career Community. http://insidetech.monster.com/news/articles/5367-report-shortage-of-cyber-experts-a-big-threat-to-us-government (accessed April 9, 2010).
[44] Sawyer, David. "The Joint Doctrine Development System." *Joint Force Quarterly*, Dec. - Jan.1997, 3.

[45] Harnessing the intellectual capital and focus on developing a new form of orientation known as "cyber-mindedness." Similar to the concept of "air-mindedness" already imbued into every Airman, cyber-mindedness involves the unhindered development of cyberspace capabilities to achieve desired effects. Derived from Lt Col Sebastian M. Convertino II, CDR Lou Anne DeMattei, and Lt Col Tammy Knierim, *Flying and Fighting in Cyberspace*, Maxwell Paper no. 40 (Maxwell AFB, AL: Air University Press,July 2007), 9.
[46] U.S. Strategic Command, "Fact Sheet on Joint Task Force-Global Network Operations. http://www.stratcom.mil/factsheets/gno/Joint_Task_Force_-_Global_Network_Operations (accessed 3 April 2010).
[47] Gates, Robert. *2010 Quadrennial Defense Review Report*. Washington, DC: Department Of Defense, 2010, 37-38.

BIBLIOGRAPHY

Alberts, David S. *Understanding Command and Control (Future of Command and Control).* Georges: Ccrp Publication Series, 2006.

Alexander, Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly,* Issue 46. (3rd Quarter 2007): 58-61.

_____. "Advance Questions for Lieutenant General Keith Alexander, USA." armed-services.senate.gov. armed services.senate.gov/statemnt/2010/04%20April/ Alexander%2004-15-10.pdf (accessed April 16, 2010).

C. Robert Kehler, General, USAF Commander, AFSPC. *The United States Air Force Blueprint for Cyberspace.* November 2, 2009.

Crowell, Richard M. War in the Information Age: A Primer for Cyberspace Operations in the 21st Century (Newport, RI: Naval War College, 2008).

Charney, Scott, James R. Langevin, Michael T. McCaul, and Harry Raduege. *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008.

Chilton, Kevin P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities." *Air and Space Power Journal* XXIII, Number. 3. (Fall 2009): 5-10.

Gates, Robert. *Quadrennial Defense Review Report*. Washington, DC: Department Of Defense, 12 February 2010, 37-38.

_____. *Unified Command Plan 2008*. Washington, DC: DOD, 2008.

Libicki, Martin C. "Cyber deterrence and Cyberwar." *Rand.org*. www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (Accessed April 3, 2010)

Machiavelli, Niccolo. "VI." In *The Prince and The Discourses (Modern Library No. 65).* New York: Modern Library 1950: 21.

McCullough, Barry. "U.S. Fleet Cyber Command." Speech. Mission Brief from U.S. Tenth Fleet, Maryland, February 22, 2010.

Messmer, Ellen. "U.S. cyber counterattack: Bomb 'em one way or the other." NetworkWorld.com. http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html (accessed April 9, 2010).

Nakashima, Ellen, and Brian Krebs. "Private companies outbid Uncle Sam for Cyber Warriors" Houston Chronicle.

http://www.chron.com/disp/story.mpl/business/6787376.html (accessed April 9, 2010).

Newman, David, Major, USAF. Interview by author. Personal interview. Naval War College Library, February 26, 2010.

Sawyer, David. "The Joint Doctrine Development System." *Joint Force Quarterly*, Dec. - Jan. 1997.

U.S. Department of Defense. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations.* Washington DC: Office of the Secretary of Defense, 23 June 2009.

_____. *Quadrennial Roles and Missions Review Report.* Washington, DC, January 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States.* Joint Publication (JP) 1. Washington, DC: CJCS, 02 May 2007 Incorporating Change 1 20 March 2009.

_____. *Department of Defense Dictionary of Military and Associated Terms.* (JP) 1-02. Washington, DC: CJCS 12 April 2001 As Amended Through 19 August 2009.

_____. *Joint Operations.* Joint Publication (JP) 3-0. Washington, DC: CJCS, 17 September 2006 Incorporating Change 1, 13 February 2008.

_____. *Close Air Support.* Joint Publication (JP) 3-09.3. Washington, DC: CJCS, 8 July 2009.

_____. *Joint Task Force Headquarters.* Joint Publication (JP) 3-33. Washington, DC: CJCS**,** 16 February 2007.

_____. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I.* Joint Publication (JP) 3-08. Washington, DC: CJCS**,** 17 March 2006.

_____. *Information Operations.* Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

_____. *Space Operations.* Joint Publication (JP) 3-14. Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 6 January 2009.

_____. *Joint Operation Planning.* Joint Publication (JP) 5-0. Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 26 Dec 2009.

_____. *The National Military Strategy for Cyberspace Operations*. Washington, DC: CJCS, December 2006. Document is now declassified.

U.S. Strategic Command, "Fact Sheet on Joint Task Force-Global Network Operations. http://www.stratcom.mil/factsheets/gno/Joint_Task_Force_-Global_Network_Operations (accessed 3 April 2010).

Vego, Milan. *Joint Operational Warfare: Theory & Practice*. Newport, RI: Naval War College Press, 2007.

Zqaniecki, Andrzej. "Online Crime Hit a Record High of More Than 27,000 in The United States." *News Blaze*, 29 September 2009. http://newsblaze.com/ (accessed 20 March 2010).